(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 102 04 870 A 1**

(51) Int. Cl.[7]:
B 44 F 1/12
B 42 D 15/10
G 07 D 7/00

(21) Aktenzeichen: 102 04 870.3
(22) Anmeldetag: 6. 2. 2002
(43) Offenlegungstag: 14. 8. 2003

DE 102 04 870 A 1

(71) Anmelder:
Infineon Technologies AG, 81669 München, DE

(74) Vertreter:
Epping, Hermann & Fischer GbR, 80339 München

(72) Erfinder:
Janke, Marcus, 81539 München, DE; Laackmann, Peter, Dr., 81541 München, DE

(56) Entgegenhaltungen:

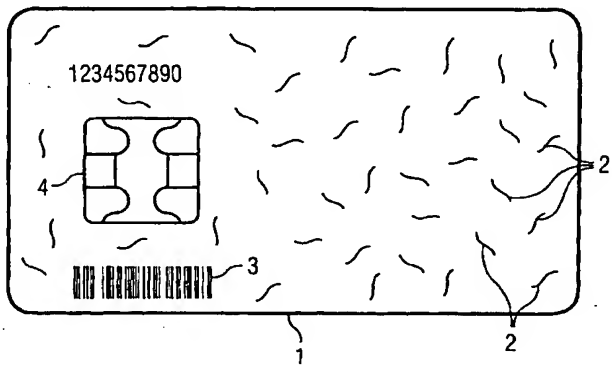
DE	197 35 628 C2
DE	196 54 607 A1
DE	33 35 678 A1
DE	28 26 469 A1
DE	24 58 705
DD	1 57 029
EP	03 64 029 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Fälschungssicherung eines Wertträgers, Wertträger und Verfahren zur Überprüfung seiner Echtheit

(57) Verfahren zur Fälschungssicherung eines Wertträgers, insbesondere einer Banknote, eines Ausweises, eines Sicherheitspapiers, einer Aktie oder einer Chipkarte, gekennzeichnet durch die Verfahrensschritte:
- Anbringen eines Sicherheitsmerkmales (2) mit zufällig verteilten Merkmalen,
- definierte Erfassung von individuellen Parametern des Sicherheitsmerkmales (2),
- Codierung der Parameterdaten und
- Aufbringen des resultierenden Codes auf den Wertträger (1).



DE 102 04 870 A 1

TRANSLATION OF PARAGRAPHS [26] – [29] OF DE 102 04 870 A1

[26] As an example, an accordingly formed value carrier indicated by reference numeral 1 in Fig. 1 is shown in the drawing as a value carrier for executing the methods according to the invention. The carrier may consist of paper or a plastic film. In principle, there is no restriction concerning the material of the carrier 1. The carrier is provided with a security feature having randomly distributed features. The security feature may consist of fibers inserted into the carrier material. The fibers are randomly distributed over the entire area of the carrier 1 and exhibit different lengths, thicknesses and colors. The randomness is caused by the fact that the fibers are inserted into the base material of the carrier at manufacturing time whereby an individual arrangement of the fibers of each value carrier is obtained. Thus, the positions of the individual fibers and both, their numbers and relative distances, are different.

[27] Further, a code is applied to the value carrier, which code has either the form of a bar code 3 (in Klarschrift ?) or of a machine readable information stored in a memory chip 4. The bar code 3 may be visibly arranged on the value carrier 1. Preferably, the bar code is not visible for the human eye and formed in a way so that it is only detectable by irradiation with light of a certain wavelength. This could for example be realized by using ultraviolet- or infrared-active colors. Alternatively or additionally the code could also be stored in the memory chip 4. The memory chip 4 is shown in the figure as a so called chip module with external contacts. Access to the information could therefore occur by contacting the visible contact areas. If the chip module or the value carrier, respectively, has an antenna for data transmission, reading out the code could also occur contactless.

[28] Additionally, the value carrier contains an identification feature 5 which is shown as serial number in the figure. The serial number could also comprise the name of the owner of the value carrier and additional information such as address or date of birth. Preferably, the information of the identification feature is included into the coding of the parameter data obtained from the security feature.

[29] By the singleness of the security feature 2 formed by fibers in the present invention, i. e. by its singular structure, a reproduction of the value carrier is practically impossible. A falsification of the value carrier is only possible if the falsifier knows the secret key for encoding the parameter data, by which he is enabled to produce a valid falsification with a different distribution of the security feature.

****

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Fälschungssicherung eines Wertträgers, einen Wertträger und ein Verfahren zur Überprüfung der Echtheit eines Wertträgers.

[0002] Wertträger wie z. B. Banknoten, Ausweise, Sicherheitspapiere, Aktienpapiere oder Chipkarten, werden durch eine Vielzahl von Sicherheitsmerkmalen gegen Fälschung gesichert. Die Sicherheitsmerkmale werden durch aufwendige Druckverfahren oder andere Herstellungsprozesse aufgebracht. Sie können jedoch durch moderne Techniken mehr oder minder einfach reproduziert werden.

[0003] Hologramme, Wasserzeichen, Durchsichtregister, Metallstreifen, Druckbilder, die erst durch Bestrahlen mit Licht einer bestimmten Wellenlänge detektierbar gemacht werden können, usw. bieten zwar einen hohen Schutz gegen gängige Reproduktionsverfahren wie das Photokopieren bis hin zu aufwendigen Druckverfahren. Steht jedoch eine Reproduktions-Technik für die genannten Sicherheitsmerkmale zur Verfügung, so können diese auf Grund ihrer identischen Ausführung beliebig oft gefälscht werden. Viele der genannten Sicherheitsmerkmale werden deshalb in Kombination auf einen Wertträger aufgebracht um den Aufwand einer Fälschung zu erhöhen.

[0004] Weiterhin ist es bekannt, auf einem Wertträger Sicherheitsmerkmale mit zufällig verteilten Merkmalen vorzusehen. Aus der DE 197 35 628 C2 ist ein Verfahren zur Fälschungssicherung eines nicht personengebundenen Zugangsberechtigungsmittels bekannt, bei dem strukturiertes pflanzliches oder tierisches Material, wie gewachsen, an dem Zugangsberechtigungsmittel angebracht wird. Die Eigenschaften dieser Materialien bestehen darin, daß dessen Struktur in makroskopischem Maßstab weitgehend zufällig ist, so daß es sich jeweils um eine Art "biogenen Fingerabdruck" handelt, der hinsichtlich seiner charakteristischen individuellen Strukturparameter, d. h. Gestalt- und Materialparameter, absolut einzigartig ist. Derartige individuelle Parameter werden nach einem vorab definierten Meßverfahren mittels entsprechender Meßverfahren zerstörungsfrei erfaßt. So wird mittels optischer Meßverfahren der Umriß eines Blattes sowie die Nervatur in ausgewählten Bereichen aufgenommen. Die auf diese Weise gewonnenen, charakteristischen Parameterdaten werden extern als Datensätze in Computer-Datenbanken abgespeichert. Die Verifikation des nicht Personen bezogenen Zugangsberechtigungsmittels erfolgt durch eine erneute, definierte Messung der durch die Erfassung vorgegebenen Parameter. Der anschließende Vergleich der bei diesem Lesevorgang ermittelten Parameterdaten mit den zuvor erfaßten, gespeicherten Datensätzen läßt eine eindeutige Identifizierung zu.

[0005] Auch wenn das beschriebene Verfahren einen hohen Grad an Fälschungssicherung bietet, so weist es für die Praxis doch erhebliche Nachteile auf. Das Anbringen von strukturiertem pflanzlichen oder tierischen Material dürfte in der Praxis bei der Herstellung von Wertträgern in großem Maßstab nicht handhabbar sein. Insbesondere ist das Aufbringen von strukturiertem pflanzlichen oder tierischen Material auf Banknoten wohl kaum vorstellbar. Zum Anderen erfordert die Verifikation des Wertträgers einen Zugriff auf externe Computer-Datenbanken. Zur Verifikation ist somit eine Verbindung zu der Computer-Datenbank notwendig, die sich üblicherweise an einem anderen Ort befindet, an welchem die Verifikation stattfindet. Im Falle einer Leitungsunterbrechung zu der Computer-Datenbank kann eine Verifikation folglich nicht erfolgen.

[0006] Daraus ergibt sich die Aufgabenstellung für die vorliegende Erfindung, ein Verfahren zur Fälschungssicherung eines Wertträgers zur Verfügung zu stellen, welches auf einfachere Weise eine Fälschungssicherheit bietet. Weiterhin soll ein nach dem erfindungsgemäßen Verfahren hergestellter Wertträger angegeben werden. Zuletzt liegt der Erfindung die Aufgabenstellung zu Grunde, ein Verfahren zur Überprüfung der Echtheit des erfindungsgemäßen Wertträgers zur Verfügung zu stellen.

[0007] Ein Verfahren zur Fälschungssicherung eines Wertträgers ist durch die Merkmale des Anspruches 1 gegeben. Ein gegen Fälschung gesicherter Wertträger ist dem Anspruch 10 entnehmbar. Das Verfahren zur Überprüfung der Echtheit des Wertträgers ist durch die Merkmale des Anspruches 15 definiert. Vorteilhafte Ausgestaltungen ergeben sich jeweils aus den abhängigen Ansprüchen.

[0008] Das Verfahren zur Fälschungssicherung eines Wertträgers umfaßt die folgenden Schritte:

- Anbringen eines Sicherheitsmerkmales mit zufällig verteilten Merkmalen,
- definierte Erfassung von individuellen Parametern des Sicherheitsmerkmales,
- Codierung der Parameterdaten, und
- Anbringen des resultierenden Codes an dem Wertträger.

[0009] Erfindungsgemäß wird ein an sich bekannter Wertträger, z. B. eine Banknote, ein Ausweis, ein Sicherheitspapier, eine Aktie oder eine Chipkarte, mit einem einzigartigen Sicherheitsmerkmal versehen. Nach der definierten Erfassung der individuellen Parameter werden die Parameterdaten, vorzugsweise durch ein Verschlüsselungsverfahren, codiert, so daß auch bei Kenntnis des Meßverfahrens zur Erfassung der individuellen Parameter kein Rückschluß auf den auf dem Wertträger aufgebrachten Code gezogen werden kann. Der auf dem Wertträger aufgebrachte Code ermöglicht in vorteilhafter Weise die Verifikation des Wertträgers, ohne daß ein Zugriff auf in einer externen Computer-Datenbank gespeicherte Parameterdaten erfolgen müßte. Der besondere Vorteil des erfindungsgemäßen Verfahrens besteht darin, daß die aus den individuellen Parametern des Sicherheitsmerkmales ermittelten Parameterdaten nicht in einer Computer-Datenbank abgespeichert werden brauchen.

[0010] Gemäß einem vorteilhaften Schritt des erfindungsgemäßen Verfahrens umfaßt das Anbringen des Sicherheitsmerkmales das Einbringen von Fasern in den Wertträger, die durch Bestrahlen mit Licht einer bestimmten Wellenlänge detektierbar gemacht werden können. Das Einbringen derartiger Fasern ist beim Schöpfen des Papiers einer Banknote bekannt. Die Fasern bilden ein Sicherheitsmerkmal mit zufällig verteilten Merkmalen. Bislang wird nur das Vorhandensein der Fasern überprüft, indem z. B. mit einer UV-Lampe die Banknote bestrahlt wird. Erfindungsgemäß ist vorgesehen, die Fasern in einen beliebigen Wertträger einzubringen und die zufällig verteilten Merkmale mittels eines Sensors, z. B. einer CCD-Kamera mit UV- oder IR-Beleuchtung zu detektieren. Die zufällige Verteilung der vorhandenen Merkmale ist bei jedem Wertträger individuell und kann praktisch nicht gezielt reproduziert werden. Nur wenn ein Fälscher Kenntnis über das Verschlüsselungsverfahren besäße, könnte eine nicht erkennbare Fälschung mit einer anderen Verteilung hergestellt werden, die den korrekten Code aufweist. Die Herstellung eines fälschungssicheren Wertträgers erfordert auf Grund der bekannten Technologie nur einen geringen bzw. nicht vorhandenen Zusatzaufwand, aus welchem ein einmaliges Sicherheitsmerkmal resultiert.

[0011] Gemäß dem folgenden Schritt des erfindungsgemäßen Verfahrens werden als individuelle Parameter Strukturparameter des Sicherheitsmerkmales erfaßt. Solche

Strukturparameter stellen beispielsweise die Position, die Länge, die Ausrichtung, die Dicke, relative Abstände sowie die Farbe der in den Wertträger eingebrachten Fasern dar. Die Strukturparameter werden nach vorab definierten Meßverfahren zerstörungsfrei erfaßt.

[0012] Vorzugsweise erfolgt die Erfassung der Parameter mit einem biometrischen Verfahren. Biometrische Verfahren sind aus dem Bereich der Sicherheitstechnik zur Benutzeridentifizierung bekannt. Ein biometrisches Identifizierungsverfahren ist ein Verfahren, das auf der Grundlage von einzigartigen, individuellen und biologischen Merkmalen eine Person eindeutig identifizieren kann. Bekannte physiologische Verfahren sind die Analyse des Gesichtes, der Iris, der Netzhaut, der Handgeometrie oder des Fingerabdruckes. Erfindungsgemäß ist vorgesehen, diese Algorithmen zur Auswertung der Strukturparameter des Sicherheitsmerkmales einzusetzen. Grundsätzliche Prinzipien biometrischer Verfahren sind beispielsweise aus dem Lehrbuch von Rankl, Effing; Handbuch der Chipkarten, Hanser-Verlag; 3. Auflage; 1999; Seite 458 ff. beschrieben. Biometrische Verfahren können mit automatisierten Meßeinrichtungen durchgeführt werden und sind mit hoher Genauigkeit reproduzierbar, so daß der anschließende Vergleich der bei diesem Lesevorgang ermittelten Parameterdaten mit den zuvor erfaßten und auf dem Wertträger abgespeicherten Code eine eindeutige Identifizierung zuläßt.

[0013] In einer vorteilhaften Weiterbildung wird in die Codierung, d. h. nach der Ermittlung der individuellen Parameterdaten, ein dem Wertträger zugeordnetes Identifikationsmerkmal einbezogen. Das Identifikationsmerkmal kann beispielsweise die Seriennummer des Wertträgers oder der Name, die Adresse und das Geburtsdatum des Inhabers des Wertträgers darstellen. Jedes der Identifikationsmerkmale, das beispielsweise sichtbar auf dem Wertträger aufgebracht sein kann, läßt eine eindeutige Identifizierung des Wertträgers zu. Das Einbeziehen dieses einmaligen Merkmales in die Codierung verringert die Wahrscheinlichkeit, daß ein Betrüger Rückschlüsse von dem auf dem Wertträger aufgebrachten Code und der Anordnung der individuellen Parameter des Sicherheitsmerkmales auf die Codierung bzw. das Verschlüsselungsverfahren schließen kann. Das in die Codierung einbezogene Identifikationsmerkmal kann ebenfalls ein aus dem Bereich von Sicherheitspapieren (z. B. Banknote) bekanntes Sicherheitsmerkmal sein, wie z. B. magnetische Tinte, Feindruck, Wasserzeichen o. ä. Diese Sicherheitsmerkmale sind hinsichtlich Vorhandensein, Verteilung usw. auswertbar.

[0014] Zur weiteren Erhöhung der Sicherheit wird die Verschlüsselung vorzugsweise mit einem asymmetrischen Verschlüsselungsverfahren durchgeführt. Dies können beispielsweise die aus dem Stand der Technik bekannten RSA- bzw. ECC (elliptic curve cryptography)-Verschlüsselungsverfahren sein. Geeignet wäre ebenfalls die Verwendung von Hash-Algorithmen.

[0015] Die Verschlüsselung der individuellen Parameter des Sicherheitsmerkmales erfolgt vorzugsweise unter Verwendung eines geheimen Schlüssels. Der geheime Schlüssel kann dabei den die Wertträger herstellenden Firmen von einer zentralen Stelle zur Verfügung gestellt werden. Für eine spätere Verifikation des Codes werden dann öffentliche Schlüssel benötigt, die all den Organisationen bekannt sind, die eine Überprüfung der Echtheit vornehmen.

[0016] Vorzugsweise wird der resultierende Code mit einer Algorithmus- und/oder Schlüsselkennung versehen. Wenn dieser in maschinenlesbarer Form auf dem Wertträger aufgebracht wird, so kann anhand der Algorithmus- oder Schlüsselkennung auf die Codierung geschlossen werden. Die Algorithmuskennung kann Rückschlüsse auf das verwendete Verschlüsselungsverfahren geben. Die Schlüsselkennung, die beispielsweise in Form einer Prüfziffer vorgesehen ist, läßt Rückschlüsse über die Korrektheit des aufgebrachten Codes zu. Die Schlüssel- und Algorithmuskennung sollten zur Erhöhung der Fälschungssicherheit in regelmäßigen Abständen ersetzt werden. Bei der Herstellung einer Vielzahl von wertträgern ist es weiterhin sinnvoll mehrere Versionen der Schlüssel- und Algorithmuskennung zu verwenden.

[0017] Der Code kann als Barcode, in Klarschrift, oder in einem Chip auf dem Wertträger aufgebracht sein. Vorzugsweise ist der Code nicht sichtbar angebracht. Im Falle des Barcodes oder der Klarschrift könnte der Code mittels UV- oder IR-aktiver Bedruckung aufgebracht sein. Er wäre somit nur bei Bestrahlung mit Licht einer bestimmten Wellenlänge sichtbar, ansonsten jedoch für das menschliche Auge unsichtbar.

[0018] Der erfindungsgemäße Wertträger weist ein Sicherheitsmerkmal mit zufällig verteilten Merkmalen und einen auf dem Wertträger aufgebrachten Code auf. Erfindungsgemäß beinhaltet der Code Parameterdaten des Sicherheitsmerkmales in verschlüsselter Form.

[0019] Wie eingangs bereits beschrieben, kann das Sicherheitsmerkmal aus in den Wertträger eingebrachte aktiven Fasern bestehen, die bei Bestrahlung mit Licht einer bestimmten Wellenlänge detektierbar sind. Das Sicherheitsmerkmal könnte jedoch auch in Strukturmerkmalen des Wertträgers als solchen bestehen.

[0020] Vorzugsweise ist der Code in für das menschliche Auge nicht sichtbarer Form auf den Wertträger aufgebracht. Der Code kann einmal als optisch auslesbare Information in Form eines Barcodes oder Klarschrift auf dem Mehrträger angebracht sein. Der Code könnte jedoch auch in einem in dem Wertträger vorgesehenen Speicherchip untergebracht sein, welcher sich berührungslos beim Einbringen in ein entsprechendes Lesefeld auslesen läßt. Derartige Technologien sind aus dem Bereich der Chipkartentechnik hinlänglich bekannt.

[0021] Das Verfahren zur Überprüfung der Echtheit des Wertträgers umfaßt die folgenden Schritte:

- Definierte Erfassung von Parameterdaten des Sicherheitsmerkmales,
- Codierung der Parameterdaten,
- Auslesen des auf dem Wertträger aufgebrachten Codes und
- Vergleich des ermittelten Codes mit dem auf dem Wertträger aufgebrachten und ausgelesenen Codes.

[0022] Die Verifikation des Wertträgers erfolgt also durch eine erneute, definierte Messung und gegebenenfalls Verschlüsselung der individuellen Parameter des Sicherheitsmerkmales. Mittels automatisierter Meßeinrichtungen sind diese Messungen reproduzierbar mit hoher Genauigkeit durchführbar, so daß der anschließende Vergleich der bei diesem Lesevorgang ermittelten Parameterdaten mit den zuvor erfaßten, auf dem Wertträger aufgebrachten und ausgelesenen Codes eine eindeutige Identifizierung zuläßt.

[0023] Erst wenn der Vergleich die Erfüllung von vorab definierten Koinzidenzkriterien, d. h. die Übereinstimmung der Merkmale innerhalb gewisser Fehlertoleranzen ergibt, erfolgt die Signalisierung eines korrekten Wertträgers.

[0024] Vorzugsweise erfolgt das Auslesen des auf dem Wertträger aufgebrachten Codes vor der Codierung der Parameterdaten, wobei die Codierung der Parameterdaten in Abhängigkeit von in dem Code enthaltenen Daten erfolgt. Beim Auslesen des auf dem Wertträger aufgebrachten Codes wird insbesondere die Algorithmus- und/oder Schlüs-

selkennung ausgewertet. Diese beinhalten Informationen für die erneute, definierte Messung der durch die Erfassung vorgegebenen Parameter.

[0025] Der Vergleich des ermittelten Codes mit dem ausgelesenen Code umfaßt in einer weiteren vorteilhaften Ausgestaltung das Decodieren des ausgelesenen Codes mit einem öffentlichen Schlüssel. Derartige Verschlüsselungsverfahren sind aus dem Stand der Technik bekannt. Üblicherweise werden diese Verschlüsselungsverfahren jedoch nur bei der Übertragung von elektronischen Daten zwischen zwei elektronischen Geräten eingesetzt. Die Verschlüsselung zuvor ermittelter Parameterdaten und das Abspeichern des Ergebnisses auf dem gleichen Informationsträger stellt eine neue Anwendung der bekannten Verschlüsselungsverfahren dar.

[0026] Beispielhaft ist in der Zeichnung als Wertträger zur Durchführung der erfindungsgemäßen Verfahren ein entsprechend ausgestalteter Träger dargestellt, der in **Fig.** 1 mit dem Bezugszeichen **1** versehen ist. Der Träger kann aus einem Papier oder aus Kunststofffolien bestehen. Hinsichtlich des Materiales des Trägers **1** bestehen im Prinzip keine Einschränkungen. Der Träger **1** ist mit einem Sicherheitsmerkmal **2** mit zufällig verteilten Merkmalen versehen. Das Sicherheitsmerkmal **2** kann aus in das Trägermaterial eingebrachten Fasern bestehen. Die Fasern sind über die gesamte Fläche des Trägers **1** zufällig verteilt und weisen unterschiedliche Längen, Dicken und Farben auf. Die Zufälligkeit ergibt sich auch daraus, daß die Fasern bei der Fertigung in das Ausgangsmaterial des Trägers eingebracht werden, wodurch bei jedem Wertträger **1** eine individuelle Ausrichtung der Fasern erzielt wird. Es unterscheiden sich somit sowohl die Positionen einzelner Fasern, die Anzahl der Fasern als auch deren relative Abstände.

[0027] Daneben ist auf dem Wertträger ein Code aufgebracht, der entweder in Form eines Barcodes **3** in Klarschrift oder einer in einem Speicherchip **4** enthaltenen Information maschinenlesbar ist. Der Barcode **3** kann sichtbar auf dem Wertträger **1** angeordnet sein. Vorteilhaft ist es, wenn dieser für das menschliche Auge nicht sichtbar vorliegt und beispielsweise derart hergestellt ist, daß er nur bei Bestrahlen mit Licht einer bestimmten Wellenlänge detektierbar ist. Dies könnte beispielsweise durch die Verwendung von UV- oder IR-aktiven Farben realisiert sein. Alternativ oder zusätzlich könnte der Code auch in dem Speicherchip **4** enthalten sein. Der Speicherchip **4** ist in der Figur als sogenanntes Chipmodul mit äußeren Kontakten dargestellt. Ein Zugriff auf die Informationen könnte somit durch Kontaktieren der sichtbaren Kontaktflächen erfolgen. Ein Auslesen des Codes könnte auch auf kontaktlose Weise erfolgen, wenn das Chipmodul bzw. der Wertträger über eine Antenne zur Datenübertragung verfügen würde.

[0028] Der Wertträger **1** enthält darüber hinaus ein Identifikationsmerkmal **5**, das in der Figur als Seriennummer dargestellt ist. Das Identifikationsmerkmal könnte auch in dem Namen des Inhabers des Wertträgers und zusätzlichen Angaben wie z. B. der Adresse oder dem Geburtstag bestehen. Vorzugsweise wird die Information des Identifikationsmerkmales in die Codierung der aus dem Sicherheitsmerkmal gewonnenen Parameterdaten einbezogen.

[0029] Durch die Einmaligkeit des vorliegend als Fasern ausgebildeten Sicherheitsmerkmales **2**, d. h. dessen singulärer Struktur, ist eine Nachahmung des Wertträgers praktisch unmöglich. Eine Fälschung des Wertträgers ist nur möglich, wenn der Fälscher den geheimen Schlüssel zur Verschlüsselung der Parameterdaten kennt, womit er in die Lage versetzt wird, eine gültige Fälschung mit einer anderen Verteilung des Sicherheitsmerkmales zu erstellen.

Bezugszeichenliste

1 Wertträger
2 Sicherheitsmerkmal mit zufällig verteilten Merkmalen
3 Code
4 Speicherchip
5 Identifikationsmerkmal (z. B. Seriennummer)

Patentansprüche

1. Verfahren zur Fälschungssicherung eines Wertträgers (**1**), **gekennzeichnet durch** die Verfahrensschritte:
   - Anbringen eines Sicherheitsmerkmales (**2**) mit zufällig verteilten Merkmalen,
   - definierte Erfassung von individuellen Parametern des Sicherheitsmerkmales (**2**),
   - Codierung der Parameterdaten, und
   - Anbringen des aus dem Verschlüsselungsverfahren resultierenden Codes an dem Wertträger (**1**).
2. Verfahren nach Anspruch 1 dadurch gekennzeichnet, daß die Codierung der Parameterdaten unter Verwendung eines Verschlüsselungsverfahrens erfolgt.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß das Anbringen des Sicherheitsmerkmales (**2**) das Einbringen von Fasern in den Wertträger (**1**) umfaßt, die durch Bestrahlen mit Licht einer bestimmten Wellenlänge detektierbar gemacht werden können.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß als individuelle Parameter Strukturparameter des Sicherheitsmerkmales (**2**) erfaßt werden.
5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß die Erfassung der Parameter mit einem biometrischen Verfahren erfolgt.
6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß in die Codierung ein dem Wertträger (**1**) zugeordnetes Identifikationsmerkmal (**5**) einbezogen wird.
7. Verfahren nach einem der Ansprüche 2 bis 6, dadurch gekennzeichnet, daß die Verschlüsselung mit einem asymmetrischen Verfahren durchgeführt wird.
8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß zur Verschlüsselung ein geheimer Schlüssel verwendet wird.
9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß der Code (**3**) mit einer Algorithmus- und/oder Schlüsselkennung versehen wird.
10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß der Code (**3**) in maschinenlesbarer Form auf den Wertträger (**1**) aufgebracht wird.
11. Wertträger (**1**), der ein Sicherheitsmerkmal (**2**) mit zufällig verteilten Merkmalen und einen auf dem Wertträger aufgebrachten Code (**3**) aufweist, dadurch gekennzeichnet, daß der Code (**3**) Parameterdaten des Sicherheitsmerkmales (**3**) beinhaltet.
12. Wertträger nach Anspruch 11, dadurch gekennzeichnet, daß die Parameterdaten in verschlüsselter Form vorliegen.
13. Wertträger nach Anspruch 11 oder 12, dadurch gekennzeichnet, daß das Sicherheitsmerkmal (**3**) in den Wertträger (**1**) eingebrachte aktive Fasern sind, die bei Bestrahlung mit Licht einer bestimmten Wellenlänge detektierbar sind.
14. Wertträger nach einer der Ansprüche 11 bis 13, dadurch gekennzeichnet, daß der Code (**3**) mit einer Algorithmus- und/oder Schlüsselkennung versehen ist,

anhand der das Verfahren zur Erfassung und/oder Codierung der Paramter bestimmt werden kann.

15. Wertträger nach einem der Ansprüche 11 bis 14, dadurch gekennzeichnet, daß der Code in für das menschliche Auge nicht sichtbarer Form auf dem Wertträger angebracht ist.

16. Wertträger nach einem der Ansprüche 11 bis 15, dadurch gekennzeichnet, daß der Wertträger (1) eine Banknote, einen Ausweis, ein Sicherheitspapier, eine Aktie oder eine Chipkarte darstellt.

17. Verfahren zur Überprüfung der Echtheit eines Wertträgers (1), der nach einem der Ansprüche 10 bis 14 ausgebildet ist, gekennzeichnet durch die folgenden Verfahrensschritte:

- definierte Erfassung von Parameterdaten des Sicherheitsmerkmales (2),
- Codierung der Parameterdaten, insbesondere durch ein Verschlüsselungsverfahren,
- Auslesen des auf dem Wertträger (1) aufgebrachten Codes (3),
- Vergleich des ermittelten Codes mit dem auf dem Wertträger aufgebrachten und ausgelesenen Code (3).

18. Verfahren nach Anspruch 17, dadurch gekennzeichnet, daß das Auslesen des auf dem Wertträger (1) aufgebrachten Codes (3) vor der Codierung der Parameterdaten erfolgt, wobei die Codierung der Parameterdaten in Abhängigkeit von in dem Code (3) enthaltenen Daten erfolgt.

19. Verfahren nach Anspruch 17 oder 18, dadurch gekennzeichnet, daß der Vergleich des ermittelten Codes mit dem ausgelesenen Code (3) das Dekodieren des ausgelesenen Codes (3) mit einem öffentlichen Schlüssel umfaßt.

Hierzu 1 Seite(n) Zeichnungen

Nummer: **DE 102 04 870 A1**
Int. Cl.[7]: **B 44 F 1/12**
Offenlegungstag: 14. August 2003